UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/719,303	11/21/2003	Michael Bensimon	886-011604-US(PAR)	3004

2512 7590 10/14/2009

Perman & Green, LLP
99 Hawley Lane
Stratford, CT 06614

EXAMINER	
ZIA, SYED	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
10/14/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/719,303	**Applicant(s)** BENSIMON ET AL.	
	Examiner SYED ZIA	**Art Unit** 2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03 June 2009*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1 and 3-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1 and 3-22* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

Response to Amendment

This office action is in response to correspondence sent on June 3, 2009. Claims 1, 3-22 are pending for further consideration.

Response to Arguments

Applicant's arguments filed June 3, 2009 have been fully considered but they are moot in view of new ground of the rejections.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, and 3-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haverinen et al. (U. S. Patent 7,472,273), and further in view of Mason, Jr. et al. (U. S. Patent 6,100,817).

2. Regarding Claim 1, Haverinen teaches and describes a method for establishing and

managing a trust model between an identification module and a radio terminal , said method comprising: authenticating said radio terminal by said identification module, said authenticating being carried out by radio terminal authentication arrangements that are provided either to said identification module by a mobile radio-telephony network at the time of an initialization or at the time of an updating, or to said radio terminal by the identification module; and controlling by said module at least one specific characteristic of the radio terminal , said specific characteristic being previously transmitted by radio-telephony to said identification module from a secured server of said mobile radio-telephony network (Haverinen: col.13 line 37 to col.15 line 10).

Although the system disclosed by Haverinen shows all the features of the radio terminal authentication arrangements, but Haverinen does not specifically disclose authentication key with determined expiration time period.

In an analogous art, Mason, on the other hand discloses computing environment that relates to methods and apparatus for providing radio terminal by the identification module, said radio terminal authentication arrangements present in the identification module being provided with a validity period that is limited by a determined expiration date, said authentication arrangements being comprised of at least one authentication key; (col. 4 line 49 to col.5 line 3, and col.12line 39 to 65).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Haverinen and Mason, because Mason's method of time dependent encrypting/decrypting of monitored data by using published primary keys would not only promote security structure in the system of Haverinen during receiving data from host computing devices but will also provide safeguards against attempt by unauthorized person to breach security of system.

3. As per Claim 21, Haverinen teaches and describes an identification module in a radio terminal comprising a device for memorizing at least one authentication algorithm, a calculation device for executing at least applying an authentication key to said authentication algorithm as well as at least one authentication algorithm memorized in the identification module, a communication device, a device for initiating a revocation and a revocation device for revoking said authentication key, a device for memorizing a specific characteristic of the radio terminal and a device for actuating an updating algorithm for updating said authentication key, the communication device being capable of providing at least one authentication key to the radio terminal and receiving data send from a secured server of said mobile radio-telephony network (Haverinen: col.13 line 37 to col.15 line 10).

Although the system disclosed by Haverinen shows all the features of the radio terminal authentication arrangements, but Haverinen does not specifically disclose authentication key with determined expiration time period.

In an analogous art, Mason, on the other hand discloses computing environment that relates to methods and apparatus for providing radio terminal by the identification module, said radio terminal authentication arrangements present in the identification module being provided with a validity period that is limited by a determined expiration date, said authentication arrangements being comprised of at least one authentication key; (Mason: col. 4 line 49 to col.5 line 3, and col.12 line 39 to 65).

Therefore, It would have been obvious to one ordinary skilled in the art at the time of invention to combine the teachings of Haverinen and Mason, because Mason's method of time dependent encrypting/decrypting of monitored data by using published primary keys would not only promote security structure in the system of Haverinen during receiving data from host computing devices but will also provide safeguards against attempt by unauthorized person to breach security of system.

4. Claims 3-20, and 22 are rejected applied as above in rejecting claim 1 Furthermore, the system of Haverinen and Mason teaches and describes a method of authentication and trust mode and personalization a chip card for mobile telephone system, wherein:

As per Claim 3, wherein said identification module comprises at least one of an SIM type chip card, an USIM card for third-generation networks or an equivalent card comprising in a memory the representative subscription data (Haverinen: col.10 line 66 to col.11 line 16).

As per Claim 4, wherein the identification module maintains a trust relationship with the radio terminal by generating authentication means and then by providing these authentication means to the radio terminal by secured exchange mechanisms based on authentication means initially available from the radio terminal (Haverinen: col.11 line 30 to col.13 line 16).

As per Claim 5, comprising at the time of said initialization or updating generating, carried out at least by said identification module, a trust key, said trust key being used by said module for encrypting at least data exchanged between the identification module and the radio terminal (Haverinen: col.13 line 37 to col.14 line 20).

As per Claim 6, wherein said initialization step of said authentication means is done on the initiative of the radio-telephony network, after denial of the key initiated by at least one of said module, the mobile radio-telephony network or the radio terminal, following an expiration of the validity period of the key or at the time of initialization of the identification module (Haverinen: col.13 line 37 to col.14 line 20,and Mason: col. 4 line 49 to col.5 line 3, and col.12 line 39 to 65).

As per Claim 7, wherein said authenticating comprises: utilization in the radio terminal of at least one first authentication key memorized in the radio terminal by at least on first authentication algorithm memorized in the radio terminal , said first key having a validity period limited by a predefined expiration date; utilization by the identification module of at least one second key memorized in the identification module by at least one second authentication algorithm memorized in the identification module, said second key being identical or complementary to the first key and associated with the radio terminal , said second key having a validity period limited by said predefined expiration date; comparing in the identification module the results obtained by said first and second authentication algorithms (Haverinen: col.13 line 37 to col.14 line 20 and Mason: col. 4 line 49 to col.5 line 3, and col.12 line 39 to 65).

As per Claim 8, the said authenticating comprises the utilization of said predefined expiration date (Mason: col. 4 line 49 to col.5 line 3, and col.12 line 39 to 65).

As per Claim 9, said initialization is initiated by a mobile radio-telephony network and also comprises: generation by the identification module of at least one of said first and second keys; a storage in the identification module of said second key; and transmission to the radio terminal by the identification module of said first key, said first key being encrypted by use of the trust key (Haverinen: col.13 line 37 to col.14 line 20).

As per Claim 10, wherein said comparing is done between, a response produced by said first authentication algorithm, stored in memory in the radio terminal and transmitted to said identification module and, a response result, stored in memory in the identification module, produced by said second authentication algorithm (Haverinen: col.11 line 30 to col.13 line 16).

As per Claim 11, wherein said first key is an asymmetrical private key Ks and said second key being a public key Kp complementary to the first key (Haverinen: col.14 line 21 to col.15 line 10)

As per Claim 12, wherein said first key is symmetrical, said second key stored in memory in the identification module being identical to the first key, these keys forming a single symmetrical authentication key (Haverinen: col.14 line 21 to col.15 line 10).

As per Claim 13, further comprising updating said first and second keys, initiated by the identification module prior to said predefined expiration, said updating including: authentication between the radio terminal and the identification module using said first and second keys; generation by an updating algorithm of the identification module of at least one updated key taking into account information for replacing at least one of said first and second keys; memorization in the identification module of the updated key for replacing said second key; +and transmission to the radio terminal by the identification module of the updated key analogue of said first key (Haverinen: col.14 line 21 to col.15 line 10).

As per Claim 14, wherein said updating further comprises the control of at least of one identifier of the radio terminal of the identification module ((Haverinen: col.13 line 37 to col.15 line 10)

As per Claim 15, wherein an encryption of the key is carried out for said transmission to the radio terminal of the updated key analogue of the first key, said key encryption being done by said trust key (Haverinen: col.14 line 21 to col.15 line 10).

As per Claim 16, wherein the updating step also comprises: generation by the identification module of a new trust key after said authentication between radio terminal and module; memorization in the identification module of the new trust key; transmission to the radio terminal by the identification module of the newly generated trust key (Haverinen: col.13 line 37 to col.15 line 10).

As per Claim 17, wherein said updating is completed by a verification test comprising a return transmission on the part of the radio terminal of at least one datum representative of effective receipt of data transmitted by the identification module during the updating (Haverinen: col.13 line 37 to col.14 line 20).

As per Claim 18, wherein said trust key is a symmetrical encryption/decryption key analogous to said symmetrical authentication key (Haverinen: col.14 line 21 to col.15 line 10).

As per Claim 19, wherein said trust key is an erasable session key (Haverinen: col.13 line 37 to col.14 line 20).

As per Claim 20, wherein a revocation step is carried out on the initiative of the identification module, of the radio terminal , or of the corresponding radio-telephony network, said revocation comprising the erasure in a memory of said identification module of at least said first key associated with the radio terminal (Haverinen: col.14 line 21 to col.15 line 10)

As per Claim 22, wherein said trust key is a symmetrical encryption/decryption key identical to said symmetrical authentication key (Haverinen: col.14 line 21 to col.15 line 10)

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SYED ZIA whose telephone number is (571)272-3798. The examiner can normally be reached on 9:00 to 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

sz
October 13, 2009
/Syed Zia/
Primary Examiner, Art Unit 2431